REMARKS

In response to the Office Action mailed June 22, 2006, Applicants respectfully request reconsideration. Claims 1-4 were previously pending in this application. By this amendment, Claims 1 and 3 have been amended solely to address minor informalities and/or improve readability, and not to overcome any prior art rejection. New claims 5-11 have been added. As a result, claims 1-11 are pending for examination with claims 1, 3, 5, and 8 being independent claims. No new matter has been added.

I. Amendments to the Specification

The Office Action objected to the title of the invention as not descriptive and indicated that a new title was required that would be clearly indicative of the invention to which the claims are directed, stating that the current title is imprecise.

While not necessarily agreeing with the Office Action in this regard, Applicants nonetheless have amended the title to read, "Methods and Apparatus for Randomly Adjusting Power for an Asynchronous Circuit."

Accordingly, withdrawal of this objection is respectfully requested.

II. Objections to the Claims

On page 2, paragraph 3, the Office Action objected to claims 1 and 3 for containing minor informalities.

Applicant has amended claims 1 and 3 as suggested in the Office Action. Accordingly, withdrawal of these objections is respectfully requested.

III. Rejections under 35 U.S.C. §112 ¶2

The Office Action rejected claims 1-4 under 35 U.S.C. 112, paragraph two, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicants have amended claims 1 and 3 to address the noted informalities, and respectfully request withdrawal of these rejections.

IV. Overview of Embodiments of the Invention

One embodiment described in the application is directed to methods and apparatus for masking data being processed by an integrated circuit. In this embodiment, a power consumption of the circuit is randomly distributed such that an external power analysis of the circuit is unable to reveal the nature of the data being processed by the circuit. In such methods and apparatus, the total "natural" power consumption of the circuit is first predetermined. Subsequently, power is then randomly supplied to the circuit such that the total supplied power remains essentially equivalent to the "natural" power consumption, but is provided randomly over an extended time window. Such a random redistribution of supplied power causes an external power analysis to yield a different result each time for the data being processed. In this manner, sensitive data is masked or protected against unwanted discovery. An exemplary integrated circuit implementation may employ asynchronous processing elements that, because they are not linked to a clock signal, may execute their data processing operations at the first point that the power supply is providing enough power for them to complete their operations; accordingly, the random supply of power over an extended time window does not adversely affect data processing.

The foregoing summary is provided solely for the convenience of the Examiner. It should be appreciated that each of the independent claims may not be limited in the manner described in the summary above. Therefore, the Examiner is requested not to rely upon the summary for determining whether each of the claims distinguishes over the prior art of record, but to do so based solely on the language of the claims themselves and the arguments presented below.

V. Rejections under 35 U.S.C. §112 ¶1

The Office Action rejected claim 2 under 35 U.S.C. 112, paragraph one, as failing to comply with the enablement requirement, stating that: *The specification fails to disclose that the total power is determined according to a maximum possible power consumption of the calculation element.* Applicants understand this rejection under 35 U.S.C. §112 ¶1 as being a rejection of the specification as allegedly failing to enable the subject matter of claim 2. Applicants respectively traverse this rejection.

First, Applicants draw the Examiner's attention to lines 14-16 on page 2 of the specification, which clearly and explicitly supports the notion of determining a total power provided to the calculation element according to the maximum possible power consumption of the calculation element. Applicants respectfully submit that a determination of a maximum power consumption of a circuit is well within the routine skill and knowledge of one or ordinary skill in the art.

Second, Applicants draw the Examiner's attention to Fig. 2 and the corresponding text on pages 4 of the specification. In particular, Applicants' specification reads:

> "Fig. 2 shows, by a dotted line P, what the power absorbed by circuit 1 could be in a conventional case, if said circuit was directly supplied by voltage Valim without using variable generator 2 specific to the present invention. In this case, element 1 *takes as much power as it instantaneously needs* [emphasis added]. This is what enables a possible pirate to analyze power consumption peaks and link them to the processed data (bits 0 or 1). According to the present invention, the same amount of power required for the execution of the entire calculation is randomly distributed in time in window T." (Page 4, lines 23-29).

As described in the citation, the dashed line P of Fig. 2 shows a typical, unregulated power consumption of the circuit. Based on the italicized phrase above, one of ordinary skill in the art would readily appreciate that this power consumption ranges from some nominal to maximum value that the circuit is capable of consuming. In one aspect of Applicants' disclosure, such power is randomly redistributed throughout window T such that the integrals of both curves are equivalent. Accordingly, it would also be readily appreciated by one of ordinary skill in the art that, in some instances, knowledge of the maximum possible power consumption by the integrated circuit—which is easily ascertainable using well-known techniques—is desirable for calculating how to appropriately and effectively redistribute the power supplied to the circuit. In view of the foregoing, Applicants respectfully submit that the disclosure is enabling to the extent required by 35 U.S.C. §112, paragraph one, with respect to the subject matter of claim 2. Accordingly, withdrawal of the rejection under 35 U.S.C. §112, paragraph one, is respectfully requested.

VI. Claim Rejections Under 35 U.S.C. §102

The Office Action rejected claims 1-4 under 35 U.S.C. 102(e) as allegedly being anticipated by U.S. Patent No. 6,698,662 ("Feyt"). Having amended claims 1-4 solely to address minor informalities and to overcome the objections and rejections under §112, paragraph two, Applicants respectfully traverse the rejections under 35 U.S.C. §102.

A. Overview of Feyt

Feyt discloses a method and system for masking the operations internal to an integrated circuit from attack by external power analysis (Abstract). In Feyt's system, a random signal generator is coupled to the power supply, and consumes a random or very irregular amount of power that *is added to* the power consumption of the circuit performing the real calculations (Col. 2, lines 49-51) (emphasis added). In this way, an external analysis of the power consumption shows a pattern that is unrelated to the actual power consumption of the circuit (Col. 1, lines 58-60). In an embodiment, this extra power consumption is done using an integrator to maintain the appearance of a smooth power consumption (Col. 2, lines 63-65).

B. Claims 1-2

Applicants' independent claim 1, as amended, is directed to a method for supplying an asynchronous calculation element of an integrated circuit. The method comprises randomly distributing, in a predetermined time window, an instantaneous supply power of the asynchronous calculation element, a total power in the predetermined time window being predetermined.

Feyt does not teach or suggest all the limitations of claim 1. Specifically, Feyt does not disclose predetermining a total power to be supplied within a predetermined time window, and randomly distributing an instantaneous supply power in accordance with that total power in the predetermined time window. While Feyt does teach or suggest a random signal generator varying the power draw of a circuit, there is no mention of any predetermination of power consumed or a time window. Further, Feyt does not teach using asynchronous calculation elements, as required

by claim 1. For at least the foregoing reasons, claim 1 patentably distinguishes over Feyt and is in allowable condition.

Claim 2 depends from claim 1 and is allowable for at least the same reasons.

C. Claims 3-4

Applicants' independent claim 3, as amended, is directed to a circuit for supplying at least one asynchronous calculation element of an integrated circuit. The circuit comprises a variable supply element configured to randomly distribute in a predetermined time window an instantaneous energy provided to the asynchronous calculation element, a total power in the predetermined time window being predetermined.

For reasons that should be clear from the discussion above in conjunction with claim 1, Feyt does not teach or suggest all the limitations of claim 3. Specifically, Feyt does not disclose predetermining a total power to be supplied within a predetermined time window, and randomly distributing an instantaneous energy in accordance with that total power in the predetermined time window. Further, Feyt does not teach or suggest using asynchronous processing elements, as required by claim 1. For at least the foregoing reasons, claim 3 patentably distinguishes over Feyt and is in allowable condition.

Claim 4 depends from claim 3 and is allowable for at least the same reasons.

In view of the foregoing, it is clear that no case of anticipation has been established, as there is no teaching or suggestion in the prior art of record that satisfies the limitations of the pending claims. Therefore, it is respectfully asserted that the rejection of claims 1-4 under §102 as allegedly being anticipated by Feyt is improper and should be withdrawn.

VII. General Comments on Dependent Claims

Since each of the dependent claims depends from a base claim that is believed to be in condition for allowance, Applicants believe that it is unnecessary at this time to argue the allowability of each of the dependent claims individually. Applicants do not, however, necessarily concur with the interpretation of the dependent claims as set forth in the Office Action, nor do Applicants concur that the basis for the rejection of any of the dependent claims is

proper. Therefore, Applicants reserve the right to specifically address the patentability of the dependent claims in the future, if deemed necessary.

VIII. New claims

New claims 5-11, including independent claims 5 and 8, have been added to further define Applicants' contribution to the art. Independent claim 5 recites, *inter alia*, "supplying power randomly to an asynchronous processing element so as to mask data being processed by the asynchronous processing element without adding to the power consumption of the asynchronous processing element." Independent claim 8 recites, *inter alia*, "a controller to supply power randomly to an asynchronous processing element so as to mask data being processed by the asynchronous processing element without adding to the power consumption of the asynchronous processing element." Thus, these claims also distinguish over Feyt for at least the reasons discussed above.

CONCLUSION

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue, or comment set forth in the Office Action does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Furthermore, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify any concession of unpatentability of the claim prior to its amendment.

In view of the foregoing amendments and remarks, this application should now be in condition for allowance. A notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicants' representative at the telephone number indicated below to discuss any outstanding issues relating to the allowability of the application.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicants hereby request any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Respectfully submitted,

Dated: October 23, 2006

By: *___/ Joseph Teja, Jr. /*_____

Joseph Teja, Jr.
Registration No.: 45,157
WOLF, GREENFIELD & SACKS, P.C.
Federal Reserve Plaza
600 Atlantic Avenue
Boston, Massachusetts 02210-2206
(617) 646-8396